Message Authentication, Integrity, and Non-repudiation from Paper to PKI

Introduction

Authentication, integrity and non-repudiation message practices in the paper-based environment relied on (in many cases) dozens of years of documented practices and procedures. Security features tended to be "low tech" and provided by people in well-understood processes.

With the arrival of personal computers and computer networks, people could send more messages more often more easily. In fact, electronic message programs became the Government of Canada's (GoC) main way to communicate information. Unfortunately, message authentication, integrity, and non-repudiation practices were not successfully migrated to the electronic message environment. If security was an issue, people would revert back to paper-based practices. Electronic messages were generally used for intra-governmental business using private, closed networks.

The increasing ubiquity of the Internet has contributed to the GoC's commitment to provide Canadians with on-line access to public services by 2004. More and more electronic messages will be used for external business (government to citizen , government to industry) using a public, open network. Public Key Infrastructure (PKI) is internationally recognized as an enabler for electronic business. It affords confidence in the security, privacy, and trustworthiness of electronic messages, whether transmitted over the Internet or internal corporate networks. What paper and electronic-based message authentication, integrity, and non-repudiation practices are accommodated by the GoC PKI? What practices are not accommodated and why?

This discussion and requirements document describes message authentication, integrity, and non-repudiation practices from paper through to a PKI. It highlights how these practices are enhanced using a PKI but also points out some practices that have been overlooked.

Notes

This is a draft document. Originally the intent was to solicit input from readers by posing a series of questions. Recently the focus of the document has changed. A definition of requirements for PKI-enabled applications and for digital signatures and signing as well as questions (to-date unanswered) are included.

Purpose

The intent of this document is to:

- Describe paper-based, and electronic-based message practices used for authenticity, integrity and non-repudiation;

- Describe the same practices using a PKI; and,
- Highlight issues surrounding the use of a PKI for these practices.

Once consensus has been achieved, this paper will form the basis for a Requirements Definition for digital signing and digital signatures for the GoC PKI.

Audience

Readers of this report are requested to provide solutions to problems identified, provide comments, and/or describe other issues associated with authentication, integrity and non-repudiation of messages in a PKI.

Please direct questions, comments, and suggestions to:

Paul van Vlerken
Executive Services Officer
GoC PKI Secretariat
Chief Information Officer Branch of Treasury Board Secretariat
6th Floor, CGI Building
275 Slater St.,
Ottawa, Canada
K1A 0R5

Tel: (613) 952-1476
Fax: (613) 946-9893
E-Mail: vanvlerken.paul@tbs-sct.gc.ca

Layout

The first section of this document describes paper-based message authentication, integrity and non-repudiation practices while the second section describes the same practices for electronic messages. The third section describes the effect of a Public Key Infrastructure on electronic-based messages. The third section also examines some confidentiality practices within a PKI.

Terminology

Readable Text is information that can be read and understood by a person without the use of a transformation (e.g. encryption/decryption).

Authentication ensures that messages are what they purport to be and message originators are whom they purport to be, and that intended recipients receive the messages.

Data Integrity ensures that data is unchanged from its source and has not been accidentally or maliciously altered.

Non-repudiation ensures that strong and substantial evidence is available to the sender of message that the message has been delivered, and to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the message. This includes the ability of a third party to verify the integrity and origin of the message.

Confidentiality ensures that information can be read only by authorized entities.

Section 1: Paper-based Messages

This section describes paper-based authentication, data integrity, and non-repudiation practices. In this environment, a message is a communication between two parties. The message consists of a cover (e.g. a memorandum, minute cover page) and/or attachments (documents physically attached to the cover) and/or enclosures (documents included with the cover). The message is normally sent within a container (e.g. envelope, file folder).

A paper-based message is one that is sent on paper.

A hand-written signature is the visible output of a manual signing process.

Paper-based Authentication Practices

- Message container has distinguishing pre-set marking (e.g. return address of sender, logo or other identifier of sender);
- Sender and recipient names and addresses can be authenticated to a certain extent using other means (e.g. telephone books, postal code or zipcode guides, address layout protocols – name, street, province/state, country);
- Message is sent via a trusted carrier (e.g. Canada Post, Courier, Internal Mail, delivery in person);
- Message container or message is date and/or time stamped (postmark). The postmark contains the location of the originating trusted carrier site as well as a trusted date and time;
- Covers, attachments and enclosures contain features such as; a footer or header with the document creation information on every page, a watermark, a seal, letterhead, and pagination (e.g. 1 of 10 pages); and,
- Covers, attachments and enclosures are signed (see below).

Paper-based Data Integrity Practices

- Message container is sealed;
- Message is sent via a trusted carrier (e.g. Canada Post, Courier, Internal Mail, delivery in person);
- Message container has return instructions (e.g. if not delivered within 7 days ...);
- Message is stored in a secure place before sending (e.g. a Canada Post box);
- Message is stored in a secure place before a recipient collects it (e.g. individual mail box);

- Attachments are physically attached as a part of the message (e.g. stapled);
- Covers, attachments and enclosures contain features such as a footer or header with the document creation information on every page, a watermark, a seal, letterhead, and pagination (e.g. 1 of 10 pages);
- Covers, attachments and enclosures are signed (see below); and,
- Covers contain information concerning accompanying attachments and enclosures.

Paper-based Non-repudiation Practices.

- Message container has distinguishing pre-set marking (e.g. return address of sender, logo or other identifier of sender);
- Message container has one recipient address;
- Message is sent via a trusted carrier (e.g. Canada Post, Courier, Internal Mail, delivery in person);
- Message can be sent via registered mail whereby the receiver must sign for the message;
- Message has return instructions (e.g. if not delivered within 7 days ...);
- Message container or message is date and/or time stamped by a trusted source (postmarked);
- Message is accompanied by a transmission slip that is signed (see below) and returned by the recipient to the sender;
- Cover, attachments and enclosures contain dates (e.g. creation). Creation and other dates are important as they may differ from the postmark date;
- Covers, attachments and enclosures contain features such as a footer or header with the document creation information on every page, a watermark, a seal, letterhead, and pagination (e.g. 1 of 10 pages);
- Messages are received by specifically assigned sections within an organization. The messages are logged and then forwarded to the applicable people. The receipt function and the message opening and answering function are performed by different people; and,
- Covers, attachments and enclosures are signed (see below).

Signatures.

Signed messages strengthen authentication, data integrity and non-repudiation. A signature is the visible output of a signing process.

- A signature is usually accompanied by a signature block which includes other identifying information (e.g. the name of the originator in printed form, telephone number, job title etc.);
- A signature may have different forms - initials, given name only, complete signature;
- It is a common practice for a person to sign on behalf of someone else – generally the person authorized to sign. In this case the signature does not relate to the signature block;
- A complete signature usually denotes a document of more importance or value than documents signed with initials or just a given name or no signature at all;
- A complete signature usually denotes that a signer has taken responsibility for the content of the document;
- A signature is considered to be unique and is believed to be timeless (a hand-written signature is verifiable and understandable for hundreds of years). The timelessness of the signature is principally due to the medium used (paper and ink) and the signing process (see next bullet);
- The practice of paper-based signing has existed for several hundred years;
- The science of signatures (recognition, style, forgery detection, implicit and explicit meanings behind the signature, usage etc.) and signing has existed for hundreds of years;
- A signature can be verified by comparing it against other messages and documents signed by the same person (e.g. specimen signature cards);
- A signature can be authenticated by having a second person "witness" the signing. The witness knows the signer and is usually held in high regard by the community (e.g. a Notary);
- A message may have numerous signatures (e.g. when a document is routed to several people each of whom adds comments and signs them or a contract requiring signatures from all parties); and,
- All pages of an important document are signed (using initials generally).

Issues

Authentication, integrity and non-repudiation issues with paper-based messages are described below:

- Enclosures are not physically attached to the rest of the message;
- The message container is not signed;
- Cover, attachments and enclosures are sent as readable text;
- Transmission slips (receipts) are not understood nor used appropriately;
- Covers, attachments and enclosures are traditionally only signed on the last page;
- Attachments can be easily detached from a message;
- The page and document format practices (watermark, pagination, headers, footers) on unsigned pages and documents can be easily duplicated or changed without detection;
- The content of the message and its subordinate parts can be changed without detection;
- Send and receipt practices can be easily duplicated or changed without detection; and,
- Signatures can be duplicated (forged) without immediate detection.

Conclusion

In general, paper-based message practices for authentication, data integrity, and non-repudiation are based on documented and well understood procedures. Normally, paper messages follow pre-defined work steps within well-documented work processes. People are appointed, assigned responsibilities and held accountable for managing messages. These practices provide a trustworthy environment.

The use of a signature is the best deterrent for message tampering. The medium (paper) and the systems used to create messages (e.g. a wordprocessor) are the weakest link in assuring message authenticity, integrity and non-repudiation, as the messages can easily be changed or substituted. However, the policies, procedures and practices in place allow for early detection of paper message tampering.

Section 2: Electronic-based Messages

This section describes electronic-based message authentication, data integrity, and non-repudiation practices. In this environment, a message is a communication between two parties. The message consists of a cover (e.g. e-mail) and/or attachments (documents included with the cover). The message is normally sent using a container (the message "envelope") which depends on the electronic messaging protocol.

An electronic-based message is one that is sent electronically using a computer network.

An electronic signature is the visible output of the electronic signing process.

Electronic-based Authentication Practices

- Message cover has distinguishing pre-set marking (e.g. return address of sender, logo or other identifier of sender);
- Sender and recipient names and addresses can be authenticated to a limited extent (less than paper) using other means (e.g. address layout protocols – name, domain server, organization type and/or name, country code);
- Message may be sent via a trusted carrier (e.g. a private telecommunications network). More often, messages are sent via an non trusted carrier (Internet);
- Message container or message is date and/or time stamped using a non-trusted source (e.g. the PC or server clock);
- Covers and attachments contain features such as: a footer or header with the document creation information on every page, an electronic watermark, electronic seals, and pagination (e.g. 1 of 10 pages). Electronic-based messages do not have enclosures although message attachments have the same characteristics as enclosures (i.e. not physically attached to the cover); and,
- Covers and attachments may be electronically signed (see below).

Electronic-based Data Integrity Practices

- Message is sent in packets and a cyclical redundancy checksum (CRC) is used to ensure the number of packets sent is equal to the number of packets received. The transport protocol includes error detection and recovery mechanisms;
- Message may be sent via a trusted carrier (e.g. a private telecommunications network). More often, messages are sent via an non trusted carrier (Internet);

- Message is stored in a secure place before sending (e.g. a secure network server). Often messages are stored for transmission on servers outside the secure network environment;
- Message is stored in a secure place before a recipient collects it (e.g. individual mail box on a secure network server);
- Attachments are embedded as a part of the message;
- Covers and attachments contain features such as a footer or header with the document creation information on every page, a watermark, a seal, letterhead, and pagination (e.g. 1 of 10 pages);
- Covers and attachments may be electronically signed (see below); and,
- Covers contain the file names of embedded attachments.

Electronic-based Non-repudiation Practices

- Message cover has distinguishing pre-set marking (e.g. return address of sender, logo or other identifier of sender);
- Message may be sent via a trusted carrier (e.g. a private telecommunications network). More often, messages are sent via an non trusted carrier (Internet);
- Message can be sent with receipt options set whereby the sender is aware when the message is received and when it is opened by the recipient;
- Some Message container protocols have return instructions (e.g. warn sender if message undelivered after four days...);
- Message container or message is date and/or time stamped;
- Cover and attachments contain dates (e.g. creation);
- Covers and attachments contain features such as a footer or header with the document creation information on every page, a watermark, a seal, letterhead, and pagination (e.g. 1 of 10 pages); and,
- Covers and attachments may be electronically signed (see below).

Electronic Signatures

Signed messages strengthen authentication, data integrity and non-repudiation. A signature is the visible output of a signing process.

- An electronic signature may have different forms. For example an image of an originator or sender's signature is affixed to the Electronic Cover (known as a Graphics Signature), or the sender indicates that a paper-based duplicate message exists and was signed (often //Signed// is used to denote this practice) or the sender includes an electronic "banner" which may or may not include a graphics signature;
- An electronic signature is rarely used as it was assumed from the message "header" that the message originated from a particular person and trust was placed in this information;
- A signature is usually accompanied by a signature block (banner) which includes other identifying information (e.g. the name of the originator in printed form, telephone number, job title etc.); and,
- A signature may have different forms - initials, given name only, complete signature – these are generally represented as text from a word processor (e.g. PVV, Paul, Paul van Vlerken).

Issues

Authentication, integrity and non-repudiation issues with electronic-based messages are described below:

- Attachments are not physically bound to the message;
- The message container is not signed;
- Cover and attachments are normally sent as readable text;
- Date/Time stamp is easily altered;
- Attachments can be easily detached from a message;
- The page and document format practices (watermark, pagination, headers, footers) on unsigned pages and documents can be easily duplicated or changed without detection;
- The content of a message can be easily changed without detection;
- Send and receipt practices can be easily duplicated or changed without detection;
- Signatures can be duplicated (forged) without immediate detection;
- Messages are being sent through public, non-trusted networks;

- Because of the inadequacy of electronic-based processes (especially signing practices), users have to revert back to paper-based practices resulting in two copies of the same transmission; and,

- The return receipts of the message are not signed.

Conclusion

In general, the process of signing which had persisted in our culture for hundreds of years was not migrated successfully to the electronic-based message environment. In fact, most electronic messages are never signed yet often they are the source for numerous decisions within organizations including the Government of Canada. Some electronic signing practices have been adopted; however, they are neither universally accepted nor used. These practices include "graphics-based" signatures, banners, unique email address identifiers, and replacing electronic messages with a signed paper copy as the authoritative source. Electronic documents signed with electronic signatures are not admissible as evidence in the Canadian courts unless the relevant records keeping system can demonstrate reliability.

Section 3: Electronic-based Messages using a PKI.

This section describes electronic-based message authentication, data integrity, and non-repudiation practices within a PKI. Most practices address deficiencies in the paper-based and electronic-based (before PKI) environments. Many of the practices within a PKI have created issues. Proposed requirements are described in an attempt to address the issues.

In this environment, a message is a communication between two parties. The message consists of a cover (e.g. e-mail) and/or attachments (documents included with the cover). The message is normally sent using a container (the message "envelope") which depends on the electronic messaging protocol. The message is sent using encryption and/or digitally signing processes.

An electronic-based message is one that is sent electronically using a computer network.

An electronic signature is the output of the electronic signing process. The electronic signature may no longer be visible output.

A secure electronic signature is the output of a secure electronic signing process.

A digital signature is a type of secure electronic signature that uses a PKI digital signing process.

What has changed?

What are the environmental changes that result in the requirements for a PKI?

The following changes have occurred within the last few years:

- The Government of Canada is sending electronic messages using public telecommunications networks such as the Internet;
- The Government of Canada is sending secure (higher sensitivity) electronic messages internally;
- Electronic messages are increasingly relied on for conducting business (authorizing, approving, advising, directing etc.);
- Scientific and technological innovations have been developed and implemented which enhance the confidentiality, authenticity, integrity, and non-repudiation of electronic messages;
- Once Bill C-6 is passed, electronic documents will be as valid as paper documents as admissible evidence in the Canadian courts. That is the electronic document can be the authoritative source;

- Once Bill C-6 is passed, a secure electronic signature has equal weight as a paper-based signature in the Canadian courts; and,

- The life cycle (creation to long-term storage) of electronic messages can be completely automated.

Digital Signing using a PKI – Practices, Issues, and Requirements

This section is divided in two. The first part describes specific issues with the Express 4.0a application from Entrust Technologies which is the current PKI-enabled application supporting the GoC PKI. The second part describes more generic issues. As most practices involve digital signing, both sections are devoted almost entirely to this topic.

Part 1 – Issues and Requirements, Current PKI-enabled software implementation

This part of section 3 describes authentication, data integrity and non-repudiation issues associated specifically with the implementation of Entrust Express 4.0a. Several issues have generated requirements which are also described.

Data Integrity and non-repudiation rely on hash values. Once a recipient opens an electronic message, the PKI-enabled application recalculates the hash. If the recalculated hash is equal to the original hash the recipient can be sure the message was not changed or substituted. If a digital signing process is used, the PKI-enabled application will alert a message recipient if a sender's certificate is not valid or if it is not signed by a recognized (trusted) Certification Authority (CA).

- **Issues.** Responsibility for detection of mismatched hash values (that is, invalid digital signatures) is left to the message recipient. The current implementation of the PKI-enabled application does not display a meaningful message.

- **Requirements.** The PKI application should display a meaningful message for invalid digital signatures.

Creation of duplicate files. The current implementation of the PKI-enabled application (the add-ons to the Office Automation application) creates an **.ent** file for an encrypted and/or digitally signed file. The original file (**.doc** or other) is either retained or overwritten depending on the way the PKI-enabled software is implemented.

- **Issues.** Users are not always aware that duplicate files could be created – one encrypted and one readable text.

- **Requirements.** The GoC PKI Secretariat should ensure that PKI-enabled applications are configured correctly. It is proposed they develop an Implementation Guide and a User Guide.

Same icons for Digital Signing and encryption. The current implementation of the PKI-enabled application has two different option execution icons in the messaging system – one for digital signing, one for encryption – for use by the message Sender. However the same display icon is shown in the recipient "Inbox" whether the message was digitally signed, encrypted, or both.

- **Issues.** The recipient should know, by viewing his/her Inbox list, whether the message received is digitally sign and/or encrypted.

- **Requirements.** The PKI application should have separate icons to show digital signing and encryption in recipient Inboxes.

Encrypted message is automatically signed. The current implementation of the PKI-enabled application permits users to digitally sign and encrypt a message, digitally sign a message, or encrypt a message. The authenticity of the sender is provided through the digital signature.

- **Issues.** Are there messages where sender authentication is not required?

- **Requirements.** The default setting for the PKI-enabled application should be to digitally sign every message whether it is encrypted or not.

Digitally signing is a conscious act. To strengthen non-repudiation PKI users must consciously be aware they are digitally signing a message. Similarly, message recipients must be aware they are receiving a digitally signed message.

- **Issues.** The current implementation of the PKI system does not alert the user that a digital signing process has started or has been completed.

- **Requirements.** The PKI-enabled application should ensure the Sender of a message confirms that he/she is digitally signing the message. Furthermore, the recipient of digitally signed message should be aware that the received message had been digitally signed and by whom.

Digitally signed return receipt. To strengthen non-repudiation the recipient of a digitally signed message should in turn, digitally sign a return-receipt. Ideally the return-receipt should recite the recipient's view of exactly what was signed and the intent of the signature.

- **Issues.** The current implementation of the PKI system does not have this feature. Should it?

- **Requirements.** This issue should be investigated by the GoC PKI Secretariat.

Do I need to be a Subscriber? The current implementation of the PKI-enabled application requires the recipient of a digitally signed message to be a subscriber to the GoC PKI or a PKI cross-certified with the GoC PKI.

- **Issues.** There may be cases where message recipients only want to verify a digital signature. They do not need to subscribe to a PKI as they do not need to digitally sign or encrypt messages.

- **Requirements.** A capability should exist for users to be able to validate a digital signature without having to be a subscriber to a PKI.

Roles. A digital signature indicates a PKI user has the authority to sign the message and by doing so expect an action or actions to be carried out by the recipient (e.g. committing resources). Within the GoC the signature is associated with the signatory's business function or role. The authority to sign a message is often invested in the role not the individual.

- **Issues.** A PKI capability will exist (Attribute Certificates) which supports business roles however, the current implementation of the PKI-enabled application does not include this capability. Is role-based messaging important to you? Are Attribute Certificates the best way to support role-based business transactions in a PKI?

- **Requirements.** The PKI-enabled application system should be able to incorporate role-based messaging. That is, a message sender should be able to send a message to a role or to an individual user.

Electronic Authorization. A digital signature indicates a PKI user has the authority to sign the message and by doing so expect an action or actions to be carried out by the recipient (e.g. committing resources).

- **Issues.** Authentication of a message sender or recipient within a PKI does not include an authorization check. A user may be authenticate but not be authorized to send a message.

- **Requirements.** The PKI-enabled application should be able to validate the authority of a sender to digitally sign a message and validate the authority of a recipient to receive a digital signed message. It is proposed the PKI-enabled application inter-operate with an Automated Authorization System (AAS). The AAS would include information concerning delegations and authorities.

Signing for Another. In the paper environment signing for another was supported by well-known procedures. The person signing would be delegated the authority, to sign for or on behalf of another. A document would be signed and include the hand-written words "for" or "on behalf of" followed by the real signer's name, position, telephone number etc.

- **Issues.** This procedure has not been migrated successfully to the electronic message environment.

- **Requirements.** The PKI-enabled application should be able to verify whether an authorization has been transferred from one user to another and for how long, and authorization limitations (e.g. financial limitations). The verifications should be performed against an Automated Authorization System.

Digital signature – relationship to hand-written signatures. The digital signing process does not produce a visible or human understandable digital signature. Furthermore, a digital signature is not created nor looks like a traditional hand-written signature or graphics-based electronic signature.

- **Issues.** Hand-written signatures have been in use for hundreds of years, are PKI users able to accept digital signatures which are only understandable by computers?

- **Requirements.** The PKI-enabled application should be able to render the digital signature such that it is visible and understandable by PKI users.

Signature preservation. The digitally signed message can be made up of many parts – cover and attachments. The whole message is signed. Message attachments may be digitally signed by different people. The digital signature used to sign the whole message can be verified within the electronic messaging program.

- **Issues.** The current implementation of the PKI-enabled application does not allow a user to verify the digital signatures of message attachments within the messaging application or within the word-processing package.

- **Requirements.** The PKI application should allow users to verify digital signatures from any of the desktop software used in document creation and dissemination.

Part 2 – Issues and Requirements – generic

This part of section 3 describes generic authentication, data integrity and non-repudiation issues within the GoC PKI. Several issues have generated requirements which are also described.

Every Hash is unique. An electronic document is passed through a one way hash function that produces a large number called a hash value that is unique to the electronic document. The encrypted hash value is the digital signature.

- **Issues.** In the paper environment a hand-written signature on a document could be checked against the hand-written signature on other documents signed by the same person to validate the signature. That is, any number of documents could have the same hand-written signature. If a hash function is used, no two documents have the same digital signature. PKI-enabled applications record the output of individual digital

signing processes. They do not however provide the capabilities, especially access, storage, search and retrieval that electronic records management systems do.

- **Requirements.** An electronic records management system should be used to track hash values and relate each to the applicable digitally signed document.

Digital signing algorithms and hash functions change. Digital signing and hash algorithms will change over time. Consequently, key pairs will also change. Each message is recorded with the digital signing and hash algorithms in place at the time a message is digitally signed. The digital signing key pair is not backed up by the PKI-enabled application.

- **Issues.** This issue is very similar to existing problems with new releases of software. That is, the software's ability to read (or not) documents created with older versions of the software. In this scenario the choices were to keep all versions of the software or to migrate old data to the new format. Invariably we have always chosen to migrate the data.

  There are four choices to deal with changes in digital signing and hash algorithms. They are: keep all versions of digital signing and hash algorithms in order to recreate the event in the future; migrate messages to the new algorithms (that is re-sign and/or re-encrypt); specify a message life-cycle less than the turnover rate of the digital signing and hash algorithms; or, record the document, the hash value, and the verification certificate of the message sender.

- **Requirements.** The document, hash value, and verification certificate should be recorded together (related and inseparable) by using an electronic records management system.

Encryption algorithms change. Encryption algorithms will change over time. Consequently, the confidentiality key pair will also change. Each message is recorded with the encryption algorithm in place at the time a message is encrypted. The confidentiality key pair is backed up by the PKI-enabled application.

- **Issues.** This issue is very similar to existing problems with new releases of software. That is, the software's ability to read (or not) documents created with older versions of the software. In this scenario the choices were to keep all versions of the software or to migrate old data to the new format. Invariably we have always chosen to migrate the data.

  There are four choices to deal with changes in encryption algorithms. They are: keep all versions of encryption algorithms in order to recreate the event in the future; migrate messages to the new algorithm (that is re-encrypt); specify a message life-cycle less than the turnover rate of the encryption algorithm; or, keep a file (corporate) copy of the document in non-encrypted form.

- **Requirements.** A file copy of the document in non-encrypted form (readable text) should be kept by an electronic records management system. The electronic records management system would use an electronic registry or third party notarization service to preserve the confidentiality and reliability of the documents over time.

Electronic Registry or Third Party Notarization Service. It is required to keep documents, hash values, and verification certificates together when digital signatures are used. It is required to keep copies of encrypted documents in readable text. The documents and the associated meta-data have to be secured in an electronic records management system to ensure the authenticity and reliability of the records over time.

- **Issues.** It is proposed that an electronic registry or third party notarization service which uses PKI technology be developed and implemented. What are the legislative, policy, procedural, and technology requirements for this type of service? Note, confidentiality of recorded documents would be implemented at the record level.

- **Requirements.** This issue should be analysed by the GoC PKI Secretariat.

PKI-enabled applications change. PKI-enabled applications that manage keys and certificates will change over time. Either the same application will change versions or a completely new application will replace an existing application.

- **Issues.** This issue is very similar to existing problems with new releases of software or changes from one software to another. That is, the software's ability to read (or not) documents created with older versions of the software and/or the ability of a new software to read documents created with another software.

  Are newer versions of the same PKI-enabled application backward compatible with older versions – that is, will newer versions of the PKI-enabled application be able to manage older versions of digital signing, hash, and encryption algorithms? If the GoC PKI migrates to a new PKI-enabled application, will the new application be compatible with the old application?

- **Requirements.** Any message created with a specific version or type of a PKI-enabled software should not lose authenticity and reliability when another version or type of a PKI-enabled software is used.

Official and Committal messages. The digital signing process can be used for all messages however it is generally used for those messages where authenticity, data integrity and/or non-repudiation are required (e.g. official or committal messages).

- **Issues.** Many users do not know what are official and committal messages.

- **Requirements.** Users should be trained to manage official and committal messages.

Sensitive messages. The encryption process can be used for all messages however it is generally used for those messages of higher sensitivity (confidentiality or privacy).

- **Issues.** Many users do not know what are sensitive messages.
- **Requirements.** Users should be trained to manage sensitive messages.

When to Digitally Sign. The PKI-enabled application is integrated with messaging and word-processing applications. Digital signing and encryption are available to all PKI users and it is easy to use.

- **Issues.** Will users bother to differentiate between sensitive and other types of information? Will users know when to digitally sign or not? Is it likely that PKI users will use digital signing and encryption for all messages? If PKI users digitally sign and encrypt every message, it may cause an unnecessary burden on the PKI-enabled application, other applications such as records management systems, or networks.
- **Requirements.** PKI users should be trained to ensure the correct use of digital signatures and encryption.

Content unchanged by digital signing process. The digital signing process does not change the content of the message or any of its subordinate components. It does however add content to the message. In the paper-based environment the hand-written signature was part of the content of a message. In the PKI environment the hash value and the verification certificate are part of the content of the message.

- **Issues.** The hand-written signature is embedded in the message and consequently easily recognized as part of the content of the message. The digital signature is not embedded in the message and may be overlooked as a part of the content of an electronic message.
- **Requirements.** Electronic records management systems should be able to capture and manage the content (original document, hash value, and verification certificate) of an electronic message.

Digital signing algorithm used for encryption. Some PKIs use one key pair for both encryption and digital signing (e.g. SSL) while others separate these two functions and use two key pairs – one for digital signing and one for confidentiality. The publicly available encryption key (part of the confidentiality key pair) is backed up. Therefore PKIs that use one key pair can either backup keys or provide a secure digital signing capability (kept private). Two key schemas can provide both key backup and private signing capability.

- **Issues.** Digital signatures provide strong authentication, data integrity, and non-repudiation capabilities. The digital signature should be under the exclusive control of an individual.

- **Requirements.** The GoC PKI has chosen a two key pair system to ensure privacy, strong authentication and non-repudiation.

Sender initiation. The sender of a digitally signed message logs onto the PKI-enabled application and uses his/her signing key to digitally sign the message. The logon to the system is controlled through a password.

- **Issues.** Subscriber authentication to the PKI system is based on a password. Often password protection is not well understood or used by Subscribers. That is, for convenience subscribers delegate their passwords to colleagues or subordinates. Are we able to change user behaviour? Should user behaviour change. Is two-factor authentication required? Note, if two-factor is used, one of the factors has to be a non-transferable secret or a physical characteristic.

- **Requirements.** Two-factor authentication should not be used for GoC rudimentary, basic, and medium assurance certificates (does not apply when portability is required). Users should be encouraged to protect their passwords and not to divulge them to colleagues and subordinates.

Receiver initiation. The recipient logs onto the PKI-enabled application and uses the sender's public verification key to verify the digital signature. The logon to the system is controlled through a password.

- **Issues.** Password protection – the same issue as for Sender initiation (see above).

- **Requirements.** Two-factor authentication should not be used for GoC rudimentary, basic, and medium assurance certificates (does not apply when portability is required). Users should be encouraged to protect their passwords and not to divulge them to colleagues and subordinates.

Responsibility for message contents. A digital signature indicates a PKI user is responsible for the contents (e.g. accuracy of the information) of the message. Implicitly, responsibility is assigned to those parts of the message that a PKI user authors (creates).

- **Issues.** If a message contains attachments that are not digitally signed, is the message sender also responsible for the contents of the attachments? Should a message sender ensure that attachments are digitally signed by the document authors before their transmission?

- **Requirements.** The message sender should not be responsible for the content of attachments. Message attachments should be digitally signed. The Subscriber General Use document should include user responsibilities re: digital signing.

Multiple Signatures on the same document. In the paper environment the GoC used numerous documents (generally forms) which required to be signed by more than one signatory.

- **Issues.** The PKI applications binds all parts of a message and signs once. To enable multiple signatures there are two options. Option 1 - every time there is a signing process a new document is created and each of the signed documents in the same workflow are connected together. Option 2 - a single document is separated into one or several components each of which can be digitally signed.

  The first option requires few changes to electronic forms software but a sophisticated workflow management system to manage the collection of documents. The second option requires many changes to current electronic forms software and a few changes to workflow management systems.

- **Requirements.** Option 2 tends to be more intuitive and is recommended.

Multiple Signatures – a special case (Forwarded Email). The practice of forwarding email is a prime example of a sequential workflow. The messaging systems create a new document for each forwarding action (that is, they support option 1 above, in the section Multiple Signatures on the same document). The PKI application in this case signs the whole message and a workflow management system (if it exists) would have to keep track of each signed and forwarded message in the workflow.

- **Issues.** As above in the section Multiple Signatures on the same document, option 2 is recommended as being more intuitive. That is, the single e-mail should be separated into components – one for each forwarding action. In fact, Multi-purpose Internet Mail Extensions (MIME) supports this concept. Unfortunately very few if any of the popular messaging programs use this MIME supported feature.

  Overlaying PKI and digitally signing exacerbates the situation even though S/MIME will also support e-mail parts.

- **Requirements.** GoC messaging programs should support email separation into subordinate components as described in MIME and S/MIME. The PKI-enabled application should use this S/MIME feature to enable digitally signing of each separate message part.

Digital Signature Types. The digital signature is determined by the digital signing and hash algorithms used.

- **Issues.** In the paper environment many signature types existed (e.g. full hand-written signature, initials, first name only etc.). Often the signature type used indicated the importance of the message (e.g. a hand-written first name was applied to greetings but not to government contracts). Should there be several digital signature types? Are some digital signatures more important than others? Should the significance of a digital signing be tied to the trust placed in a certificate (e.g. basic trust indicates a lower level of significance)?

- **Requirements.** The PKI system should not have different types of digital signatures. Signature differentiation should be accommodated in the electronic Authorization System (see Electronic Authorization) and according to the value or liability of a given transaction.

Digital Signing – a shared protocol to conduct e-business. We could hypothesize that a digital signature is an accepted and understood protocol between two parties to conduct electronic business. For example, the sharing of secrets could act as a digital signing process and encryption could be used to ensure its confidentiality. That is, a digital signing algorithm and a hash algorithm may not have to be used.

- **Issues.** Is the broader definition of digital signing acceptable to GoC? Is it supported by legislation (that is, by Bill C-6)?

- **Requirements.** The GoC PKI Secretariat should analyse this issue and develop a digital signing and digital signature policy.

Authentication of PKI user (Sender). One of the strengths of a PKI is the trust relationships and the confidence placed in certificates issued under the PKI.

- **Issues.** Trust enablers include Policies, Practice Statements, User Authentication, Certificate Issuance, Key Management.

- **Requirements.** A PKI (e.g. policies, subscriber verification, technical mechanisms etc.) must provide a level of trust sufficient to verify the authenticity of PKI users before messages are digitally signed. Note, this already exists.

Witnessing. In the paper environment, strong authentication of a message sender was provided by having a trusted third party (e.g. a notary) witness the signature of the sender.

- **Issues.** The current implementation of the PKI-enabled application has no capability to support witnessing or counter-signing a signature. Should a witnessing or counter-signing practice be developed for digitally signed messages?

- **Requirements.** One of the strengths of a PKI is the trust placed in CA. This is almost the same as witnessing a signature implying that "witnessing" a signature is no longer required.

Authentication of PKI sender by recipient. The authenticity - the credentials of the message sender embedded in his/her certificate - of the digital signing process is validated when the recipient opens a message.

- **Issues.** See above – Authentication of PKI user (Sender).

- **Requirements.** A PKI (e.g. policies, subscriber verification, technical mechanisms etc.) must provide a level of trust sufficient to verify the authenticity of PKI users when digitally signed messages are received.

Non-repudiation of message (Sender). Message non-repudiation requires strong and substantial evidence and includes proof that only the sender has the private signing key, and trusted timestamps to show that the certificate was valid at the time the message was sent etc.

- **Issues.** Are PKI users able to properly manage private keys? Do we have reliable and trusted time-stamping capabilities.

- **Requirements.** User responsibilities as to the protection of private keys should be incorporated in Acceptable Use policies. Users should have sufficient training. The PKI application should have a reliable and trusted time-stamping capability.

Non-repudiation of message (Recipient). Message non-repudiation requires strong and substantial evidence and includes proof that only the intended recipient received the message, and trusted timestamps to show that the sender certificate was valid at the time the message was opened and verified etc.

- **Issues.** Do we have strong and substantial evidence that ties a PKI user, logging into the PKI application and opening a digitally signed message, to the intended recipient of the message? What are these mechanisms? Do we have a reliable and trusted time-stamping capability?

- **Requirements.** The PKI system should have mechanisms in place to provide strong and substantial evidence that a person opening a digitally signed message is the intended recipient. Note, one solution is suggested in the section Digitally signed return receipt. The PKI application should have a reliable and trusted time-stamping capability.

Time Stamping. An intrinsic part of non-repudiation is the capability to time-stamp the digital signing process, the encryption process and revocation lists. In many cases, GoC departments have specific time-sensitive information that requires a time-stamping service.

- **Issues.** What is good enough time-stamping? How do we provide trusted time-stamping services? What time sensitive information do departments handle now? Should time stamping of messages be synchronized with time stamping of CRLs and ARLs?

- **Requirements.** GoC departments should incorporate requirements for time-stamping when implementing a PKI. The requirements should apply to electronic time stamping of business level information and integration of these requirements with trusted time stamping capabilities/ frequencies in the PKI-enabled application.

Receiving Messages – Confidentiality. In the paper environment GoC executives and managers often had secretaries or clerks open their messages. The PKI system uses the public encryption key of a recipient to encrypt a message and the recipient uses his/her private decryption key to decrypt the message. For convenience executives and managers are sharing their passwords with clerks and secretaries. In this case the clerk or secretary can access the private decryption key and decrypt the recipient's message.

- **Issues.** Password sharing weakens confidentiality and the PKI. Should the practice continue? A solution could be found by using Attribute Certificates combined with an enhanced authorization framework (see Electronic Authroization).

- **Requirements.** The PKI system should include Attribute Certificates. An enhanced authorization framework (Automated Authorization System) should differentiate between the authority to open messages and the authority to action the messages.

Electronic document and records management. The PKI permits documents to remain in electronic form through their life cycle. There is no need to keep paper-based documents or copies of documents. Many GoC departments do not have electronic document and records management systems.

- **Issues.** How can departments implementing PKIs purchase and implement electronic document and records management systems? Are there other ways to manage electronic documents and PKI key usage associated with the transmission, protection, etc. of those documents and messages?

- **Requirements.** GoC departments should implement electronic document and records management systems that support key usage. The TBS Records and Documents Information Management System (RDIMS) should be enhanced to include PKI requirements.

Conclusion

In general, the Public Key Infrastructure provides such good authentication, data integrity, and non-repudiation capabilities through the digital signing process that the Government of Canada can confidently transact its business over public telecommunications networks. However many signing practices have not been considered which will require PKI-enabled application changes, integration with other systems such as electronic forms, electronic document management, electronic workflow management, and electronic records management, and changes in user behaviour.

Authentication and non-repudiation is further strengthened by the structured and comprehensive registration processes within a Public Key Infrastructure. The principle organizations within the PKI are the Certification Authorities (CAs) and Subscribers. CAs within the GoC PKI are guided by a comprehensive policy framework. Their credentials are validated during the cross certification process. Within the GoC PKI the registration of Subscribers is a rigorous process to ensure individuals (end entities) are tied to their

electronic identities (certificates). Subscriber credentials are validated every time a message is encrypted or digitally signed and sent to a recipient.